Strategy Research Project

Preparing a Cyber Security Workforce for the 21st Century

by

Colonel Robert W. Turk
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Preparing a Cyber Security Workforce for the 21st Century

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Robert W. Turk
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
William O. Waddell
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,004

14. ABSTRACT

The Department of Defense (DOD) still struggles in recruiting and training the number of qualified cyber-warriors it needs. Cyber-attacks against DOD networks continue to rise. To protect our networks and to counter future cyber-threats, the DOD must make it a priority to select, train and retain a highly skilled workforce. Currently, shortcomings in today's training and certification program undermine the DOD's ability to adequately address current threats. We do not have all the capacity and the right sets of skills to do all that is required to manage DOD networks and the evolving cyber-threat. The cyber-security workforce must evolve in order to prepare a cyber-security workforce for the 21st century. This paper examines the existing cyber-security and workforce training at the DOD and Service level and evaluates their effectiveness. It will determine if our education and training programs for cyber-professionals are synchronized across the forces. Ultimately, this study will provide recommendations on how to better prepare the cyber-security workforce for the 21st century.

15. SUBJECT TERMS
Workforce, Cyberspace, Network Operations, Information Assurance, Certification, Training

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
UU	UU	UU	UU	30	

USAWC STRATEGY RESEARCH PROJECT

Preparing a Cyber Security Workforce for the 21st Century

by

Colonel Robert W. Turk
United States Army

William O. Waddell
Center for Strategic Leadership
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Preparing a Cyber Security Workforce for the 21st Century
Report Date:	March 2013
Page Count:	30
Word Count:	5,004
Key Terms:	Workforce, Cyberspace, Network Operations, Information Assurance, Certification, Training
Classification:	Unclassified

The Department of Defense (DOD) still struggles in recruiting and training the number of qualified cyber-warriors it needs. Cyber-attacks against DOD networks continue to rise. To protect our networks and to counter future cyber-threats, the DOD must make it a priority to select, train and retain a highly skilled workforce. Currently, shortcomings in today's training and certification program undermine the DOD's ability to adequately address current threats. We do not have all the capacity and the right sets of skills to do all that is required to manage DOD networks and the evolving cyber-threat. The cyber-security workforce must evolve in order to prepare a cyber-security workforce for the 21st century. This paper examines the existing cyber-security and workforce training at the DOD and Service level and evaluates their effectiveness. It will determine if our education and training programs for cyber-professionals are synchronized across the forces. Ultimately, this study will provide recommendations on how to better prepare the cyber-security workforce for the 21st century.

Preparing a Cyber Security Workforce for the 21st Century

> Perhaps the greatest challenge faced by the Department of Defense — and the entire government enterprise — is human resources. Technological dominance is meaningless without a skilled workforce capable of operating at the highest levels of their field. In this area, we are falling short.
>
> —Rep. Jim Langevin (D-R.I.)
> Ranking Member on the House Armed Service Subcommittee on Emerging Threats and Capabilities

The Department of Defense (DOD) still struggles in recruiting and training the number of qualified cyber-warriors it needs. General Alexander, the Commander of Cyber Command and Director of the National Security Agency, has said that "at present, we are critically short of the skills and the skilled people we as a command and a nation require managing our networks and protecting U.S. interests in cyberspace."[1] Twelve years ago, I published an article, "The Army Prepares for the Next Generation of Warfare," highlighting that a possible adversary of the future could be the People's Liberation Army (PLA) and its highly trained cyber-attack units. The intent of the article was twofold. First, to explain the potential threat of the PLA and second, to inform the reader of the next generation of communication system, the Warfighter Information Network - Tactical that would provide the warfighter with the means to shoot, move, and communicate, while providing overwhelming capabilities for facilitating cyber-superiority and enabling our forces to dominate on the battlefield. One thing was omitted: the need for a highly trained and skilled cyber-warrior to run the systems and more importantly, to protect it from our future adversaries.[2]

Are we preparing our cyber-security workforce for the 21st century? Can we execute the nation's next war if we lose our ability to receive email, access the Internet, use global positioning systems or critical warfighting systems, or rely on data integrity?

Lieutenant General Mary Legere, Army Deputy Chief of Staff for Intelligence, reported that “our networks are constantly under attack and that we need an ability to respond proactively and have a cadre of cyber warriors that are highly trained to understand what they are doing and react at the speed of sound.”[3] Thus, this paper examines the existing cyber-security and workforce training at the DOD and Service level and evaluates their effectiveness. It will determine if our education and training programs for cyber-professionals are synchronized across the forces. Ultimately, this study will provide recommendations on how to better prepare the cyber-security workforce for the 21st century.

The Threat

Cyber-attacks against government agencies and businesses in the United States continue to rise, and cyber-threats will one day surpass the danger of terrorism to the United States according Robert Mueller, FBI Director.[4] One of the largest cyber-enclaves in the world is developed and maintain by the DOD: over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe.[5] The size of this computer network makes it one of the greatest targets for cyber-attacks in the world. To protect our networks and to counter future cyber-threats, the DOD must make it a priority to select, train and retain a highly skilled workforce. This priority not only benefits the DOD’s ability to operate effectively, but it also prepares a defense against exponential threats. An effective adversarial program does not require vast resources, only the technical expertise capable of attacking our critical nodes that support the battlefield’s tactical edge. In addition, the battlefield of the future will not target only military units. It will encompass non-military targets and require

an increasing responsibility for the synchronization of efforts with the private and commercial sectors to defend them.

The last decade has seen many governments building greater cyber-capabilities. Ilan Berman, Vice President of American Foreign Policy Council, said that, over the past three years, the Iranian regime has invested heavily in both defensive and offensive capabilities in cyberspace. Equally significant, its leaders now increasingly appear to view cyber-warfare as a potential avenue of action against the United States.[6] As recently as November 2012, U.S. officials specifically blamed Iranian hackers for cyber-assaults on the servers of Capital One Financial and BB&T, two of America's biggest banking institutions.[7] Since DOD networks are interconnected with other governmental and private networks, we will have to establish better cooperation and security threat information sharing with the private sector and worldwide coalition partners. The threat of the future will not always be identified by a soldier in uniform in a specific geographical location, having declared hostile intent or from clearly traceable origins of attack. There are thousands of attacks against the U.S. daily and the only way to remain dominant using our technologically advanced systems is with a team of cyber-personnel who are experts in their fields. Although the 20th century saw the U.S. dominating the air, land, sea and space domains with great success, as stated by Leon Panetta,

> Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, these possibilities also come with new dangers... the greatest danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attacks on 9/11. Such a destructive cyber terrorist attack could virtually paralyze the nation.[8]

Cyber-Warrior Training Requirements

In order to define the training requirements, one must first identify the functions and services needed. John Grimes, Former Assistant Secretary of Defense for Networks and Information Integration, Chief Information Officer, defined the cyber-security workforce (or, Information Assurance [IA] workforce) as system administrators, network operators, approving officials, privileged users, and IA personnel. These individuals operate and manage the DOD networks, investigate anomalies, mitigate network disruptions, and implement the technical and policy controls that protect U.S. systems.[9] Due to changes in how we manage DOD networks and the evolving cyber-threat, the cyber-security workforce must evolve. Army Major General John Davis, senior military adviser for cyber to the Under Secretary of Defense, stated that "every person who touches a keyboard is in some way associated with the cyber domain, because there are disciplines and standards associated with protecting against the threats that gives a more comprehensive definition of our cyber workforce."[10] In addition, the definition that we are working on now includes a wide range of functions and skills, including analytics, forensics, training, testing and evaluation, engineering, operational planning, leadership, legal, law enforcement and general users. However, given that, we do not have all the capacity and the right sets of skills to do all that is required; the DOD continues to struggle to fully empower the cyber-workforce.[11]

The DOD requires standardized user training for all personnel with access to government computers, focusing on IA and computer-based modules that evaluate comprehension with an end-of-course exam. Required annually, the exam determines access to the network and resources. The DOD mandates specific training and certification requirements, but allows each Service to develop its own cyber-force

training programs based on specific responsibilities and missions. In his testimony to Congress, General Alexander emphasized the need for joint training so that, when cyber-warriors are tasked with a mission, they are all trained to the same standards regardless of the uniform they wear.[12]

While joint training for all Services exists today, it is not mandated. The DOD and the Defense Information Systems Agency (DISA) are preparing a relatively new effort guided by the National Initiative for Cyberspace Education.[13] Henry Sienkiewicz, DISA's vice-chief of the information assurance executive, stated that "DISA's vision is to help to establish a very robust cyber security workforce development and certification program."[14] Although this revised training and certification program is vital, the DOD is currently using the cyber-security workforce training and certification program outlined in the DOD Directive 8570.1, *Information Assurance Training, Certification, and Workforce Management* and DOD 8570.01-M, *Information Assurance Workforce Improvement Program (change 3),* referred to as "the Manual."

DOD Directive 8570.1 provides the basis for an enterprise-wide solution to train, certify, and manage the DOD IA workforce. The policy requires IA technicians and managers to be trained and certified to a DOD baseline requirement. The Directive's enterprise-wide certification program accompanying the Manual identifies the specific mandated certifications. DOD 8570.01-M, originally signed in 2005, and updated in 2010 and 2012, identifies the knowledge and skill requirements for cyber-warriors and provides guidance for the identification and categorization of positions and certification of personnel conducting functions within the DOD workforce supporting the DOD Global Information Grid.[15]

Through the Manual, the DOD intends to educate cyber-security personnel with a fundamental understanding of security principles and practices, by providing for specific training and certification requirements for each category, specialty, and skill level of cyber-security personnel. [16] However, meeting such requirements will require a combination of formal training and experiential activities such as on-the-job training and continuing education.[17]

Currently, shortcomings in today's training and certification program undermine the DOD's ability to adequately address current threats.[18] Consequently, there is a growing level of concern that this program is not making the security workforce's IT environment any more secure. This concern was highlighted in the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency wherein the problem of protecting the cyber-domain deals with both quantity and quality, especially when it comes to highly technically skilled professionals:

> We not only have a shortage of cyber personnel required to effectively operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts.[19]

According to the CSIS, the current certification regime provides a "false sense of security," due in part to a focus on security processes which do not correlate with the technical skills required to recognize, prevent, and mitigate network security intrusions.[20] Daniel Castro, Senior Analyst with Information Technology and Innovation Foundation, and other DOD cyber-security managers are unconvinced of the efficacy of certification programs, calling for operationally focused training and performance evaluation to better serve cyber-security personnel.[21]

The reviews supporting the training and certification requirements as outlined in DOD 8570 are divided. Nonetheless, regardless of how the IA and cyber-community feel towards the DOD 8570 requirements, they remain a first step in achieving the skill workforce of the future. The primary objectives of the requirements are met if analysis is based solely on creating standards for workforce personnel, establishing minimum skill levels and creating a set of formal training requirements, and the establishment of certification programs. As cyber-threats have evolved, so have the training and certification requirements, including, for instance, the recent addition of the certified ethical hacker training and certification requirement.

However, according to Jim Gosler, National Security Agency (NSA) Visiting Scientist and founding director of the CIA's Clandestine Information Technology Office, only about 1000 security specialists in the United States have the skills to operate effectively in cyberspace.[22] Although the DOD is considered a leader in the cyber-professional training, additional work remains while each Service continues to develop its separate programs.

Increasingly, though, the Services' cyber-training programs are becoming joint-training opportunities, yet the concept of separate versus combined cyber-training is not at a mature enough state to gain full economy of scale. Although U.S. Cyber Command reached operational capability two years ago, the individual military Services have been hard at work building their own robust but discrete cyber-forces.[23] Thus, while each military Service is responsible for staffing and training its own forces, similar concepts are applied. Each cyber-training program or school focuses on basic cyber-training, with

other programs dedicated to intermediate and advanced training for mid-career and senior-level non-commissioned, warrant and commissioned officers.

Moreover, while DOD civilians receive some formalized cyber-training, this is conducted at the organization level and not part of the formalized training program afforded to military members. Yet training for the civilian workforce should not be overlooked since they make up the majority of the cyber-security workforce. An effective training and professional education program must include all cyber-personnel training, including the civilian workforce. The following summaries highlight current cyber-training between the Services.

The Air Force has recently transformed how it trains cyber-operations personnel. The first cyber-training comes after basic training and prior to first duty station and assignment. The Air Force has three distinct cyber-training courses (identified as levels 200, 300 and 400). At the six-year point in each cyber-airman's careers, he or she will take the 200 level course, updating existing skills and introducing new skills. After 10 years of service, cyber-personnel will take the 300 level course, focusing more on joint cyber-operations and strategic implications of cyberspace. The 400 level course is designed for officers at the lieutenant colonel and colonel level and their civilian grade equivalents, and focuses on policy issues and refreshing skills.[24]

The Army's cyber-training program mostly focuses on three areas: transport (network and perimeter security, hacking and exploitation), IT devices (Windows, voice over IP, client security, virtual environments, IT systems) and supporting subjects (cyber-law, computer forensics). The Army's Signal Center of Excellence offers multi-month cyber-defense courses for enlisted, officers and civilians. The most intensive

cyber-warrior training is the warrant officer course, established in 2009 at Fort Gordon, for experienced senior warrant officers. The Army also offers training with industry and advanced degree programs for captains and junior majors transitioning into the cyber-career field. Such training fills gaps in required skills by sending officers to work with a commercial industry partner for roughly 12 months. The advanced degree program is concentrated on information technology and cyber-security degree programs.

The Marine Corps also employs multiple levels of cyber-training. The Marines are utilizing cyber-training courses from both the Army and the Navy. Their “cyber-primer” is a two-week basic course for computer network operations planners, conducted for the Marines by the Army at Fort Belvoir, VA and their Communication-Electronics School.[25] In addition to cyber-training offered at the Marine Corps Base at Quantico, they are also sending selected personnel to the highly regarded Joint Cyber Analysis Course and the Joint Network Attack Course offered by the Navy.[26]

The Navy’s Center for Information Dominance offers two Navy ratings, or specialties, in the cyber-arena: Cryptologic Technician Network and the Information Systems Technician. The Cryptologic Technician students go through a 24-week Joint Cyber Analysis Course at the beginning of their careers. Sailors pursuing the Information Systems Technician rating go through a basic, 19-week school that includes commercial certifications, followed by a more advanced, 18-week school.[27] The Naval Postgraduate School offers a master's degree in cyber-systems and operations for officers of all Services.

All Services have made major improvements to their cyber-training programs and offer training opportunities to their sister Services. In fact, under the umbrella of the U.S.

Cyber Command, launched in May 2010, all Services have made significant progress in preparing cyber-warriors for cyber-warfare.[28] However, in a time where fiscal constraints will soon be the norm, all Services will have to re-look what training they offer in the future. Economy of scale and return on training investment via more joint training will prove the most beneficial from a financial perspective, even as it standardizes and supports the increasingly required joint force. Moreover, improvement in simulation technology and web-based cyber-laboratories offer a cost-effective way to train. These training techniques allow the DOD, the Services and the private sector to relook at the way training is conducted and help the military incorporate best practices and the latest tools into existing cyber-curricula. Through these partnerships, the Services are building on their collective knowledge and sharing classrooms—sometimes even while students are physically seated thousands of miles apart.[29] The Cyber Command Commander is pushing for the synchronization of joint training so that, when cyber-warriors are tasked with a mission, they are all trained to the same standards regardless of the uniform they wear.[30]

The DOD's strategic cyber assets (NSA, CYBERCOM and its subordinate commands, and exploit-and-attack organizations) are staffed with a highly trained cyber-workforce. However, the same is not necessarily the case for the cyber-organizations deployed around the globe at the installation, post, camp and station levels, although these are the majority of the cyber-defenders responsible for computer network defense. The 2008 cyber-attack against the DOD's classified computer networks was the most significant breach of U.S. military computers ever, highlighting

the effects of poor user training and local network defenders' ability to recognize security anomalies:

> It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary. The Pentagon's operation to counter the attack, known as Operation Buckshot Yankee, marked a turning point in U.S. cyberdefense strategy.[31]

In the above case, a properly trained user population and cyber-workforce may have prevented or at least detected the effects of the attack. However, in the 2008 cyber-attack, the cyber-security experts at the NSA only made the detection and observation of the attack after the malware began beaconing and trying to signal that it wanted to transmit its collected data. In fall 2010, Deputy Secretary of Defense William Lynn admitted that the virus had infected DOD networks and it took 14 months to sanitize it. In response, Brookings Institute Non-resident Fellow Noah Shachtman observed that "The havoc caused by agent.btz has little to do with the worm's complexity or maliciousness — and everything to do with the military's inability to cope with even a minor threat."[32] In cyber, you are only as strong as your weakest link.

Consequently, complementing training with realistic cyber-exercises will prove invaluable to readiness as well as fully operationalize cyber into the warfighting domains. There is nothing more true than the old adage of "Train as you fight." Thus, U.S. CYBERCOM has directed each Service to develop the means to model, simulate and exercise cyber-operations into their training and exercise plans. Brigadier General Bruce Crawford, Army's 5th Signal Commander posed the questions that most leaders

are looking for in dealing with cyber: “What happens when your network is down?” “How do you react when the entire network is down? There are no digital maps, there is no GPS, there is no network. What do you do?”[33] Consequently, Army Cyber Command created a cyber-opposition force battalion to test such questions. The 2nd Battalion, 1st Information Operations Command exercised this capability March 2012, when it participated in its first series of rotations at the Army’s national training centers, identifying strengths and weaknesses in Brigade and Division forces cyber protection,[34]

Army Cyber Command, like the other sub-organizations of U.S. Cyber Command, is actively involved in assessments, wargames, and exercises with other combatant commands and Army operational forces. Lieutenant General Hernandez, Commanding General U.S. Army Cyber Command, stated that his organization will increase its capacity in fiscal year 2014 to provide:

> A Cyber Opposition Force capacity to provide realistic, challenging cyberspace training in the conduct of Unified Land Operations to exercises, Home Station Training, and Combat Training Centers; increase our capability to conduct active defense of Army Networks through “Hunt Teams” that can find, fix, and mitigate currently un-detected malicious actors already inside the DoD infrastructure; provide capability to integrate cyberspace operations into Regional Army Land operations to support commanders’ tactical and operational cyber planning and integration.[35]

The Marines, serving as the executive agent, established the DOD Cyber Range in 2009 to test, train and educate the DOD workforce. This joint-capable training program allows testing for a full range of network operations, as well as computer network defense, information assurance, exploitation and attack cyber-events.[36] The Air Force is also conducting realistic cyber-training, an exercise including an opposing force whose mission was to penetrate and disrupt the computer networks of the "good guys"—or Blue Force—made up of DOD cyber-service components.[37]

However, since no specific criterion or measure can determine how successful these cyber-ranges and exercises are, senior DOD leadership can only testify that they are improving the DOD's ability to defend the network. Traditionally, the development of the best military training focuses on technical and hands-on training. The Services' training headquarters have discovered, through feedback from the field, that they had been doing it wrong. They are now looking at measuring proficiency instead of book learning.[38] For example, most military network operators receive initial technical training in formal schools focusing on delivering network services to users.[39] This training, though including some specific operating system and platform training, is dedicated to the operational and maintenance side of cyber-operation and not on threat identification and response. Thus, it is clear that, when it comes to defending a network, it is better to have a trained and experienced technician than one who is trained and highly certified.

Some experts believe that the U.S. is not doing enough to counter the cyber threat, which includes acquiring the right people to defend it. The federal government, in large part through the DOD and Department of Homeland Security (DHS), estimates that they will need about 10,000 to 30,000 additional skilled cyber-workers to meet the demands of operating the thousands of networks.[40] This urgent need for highly trained cyber-security personnel has led to educational and vocational programs across the U.S. establishing more IA, IT management, and forensic degrees. Changes in oversight and governance from the Pentagon have helped with this workforce effort, according to Alan Paller, Research Director at the SANS Institute. Paller noted that, up until about a year ago, the Defense Department focused on exactly the wrong evaluation criteria for

recruiting and maintaining its cyber–workforce: compliance with certification and accreditation paperwork rather than real-world warfighter capability.[41]

Consequently, the strategy for recruiting cyber-professionals cannot consist purely of building a force from within. It must take a comprehensive approach that starts in the education chain where it will develop our future cyber-workers at an early age. The Obama administration's release of the Comprehensive National Cybersecurity Initiative #8 increased emphasis on cyber-security training and personnel development programs.[42] However, while these are a good start, it is limited in focus and lacks unity of effort. Thus, in order to effectively ensure our continued technical advantage and future cyber-security, we must develop a technologically skilled and cyber-savvy workforce as well as an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950s, to meet this challenge.[43] Unfortunately, the U.S. has been slow to initiate the required programs to build cyber-warriors as compared to other nations. China has made developing cyber-experts a priority and, in fact, appears to be systematically building a cyber-warrior force. "Every military district of the Peoples' Liberation Army runs a competition every spring," says Alan Paller of SANS, "and they search for kids who might have gotten caught hacking."[44]

One successful cyber-program is the U.S. Cyber Challenge (USCC). This competitive program's mission is to significantly reduce the shortage in the cyber-workforce by serving as the premier program to identify, attract, recruit and place the next generation of cyber-security professionals. USCC's goal is to find 10,000 of America's best and brightest to fill the ranks of cyber-security professionals where their

skills can be of the greatest value to the nation.[45] The DOD has similar programs, including college internships, scholarships and summer hire programs for high school students.

Importantly, though, once a program recruits promising security personnel, they must be retained. Cyber-security turnover is quite high as personnel gain experience and security certifications and seek employment for greater pay and promotions. The main reasons and contributing factors deal with the current government civilian pay freeze and the qualification and certification mandates outlined in DOD 8570.01-M which requires new contractor hires to meet the qualification requirements when hired and obtain certifications within six months of being appointed.[46] However, in 2012, General Alexander testified that the fear of military cyber-personnel leaving for higher paying civilian jobs did not materialize.[47] Vice Admiral Michael Rogers, Commander of the Navy's Fleet Cyber Command and Lieutenant General Michael Basia, Air Force Chief Information Officer also concurred for their Services. Nonetheless, while the DOD retention numbers have remained high, as the economy continues to rebound, so will the demand for cyber-security personnel in private industry. These factors contribute greatly to skilled personnel taking jobs and moving quickly for more pay, and/or responsibility. Essentially, the DOD is competing with defense contractors and private sector IT firms for highly skilled cyber-personnel. According to Wanted Analytical and ClearanceJobs.com, the U.S. has seen an 11 percent annual increase since 2010 for cyber-professionals. This high demand will require DOD to develop creative ways to recruit and incentives retention efforts.

DOD's Way Forward

To further complicate an already-complex cyber-environment, the DOD's role will have to change, not only internally but also externally via coordination with other government agencies. The Department of Defense, in large part through the capabilities of the NSA, has developed the world's most sophisticated system to detect cyber-intruders and attackers.[48] This capability supports information sharing with the DHS, which is responsible for domestic cyber-security and coordination with the private sector and the Federal Bureau of Investigation, which handles the investigation of cyber-attacks once they take place.

Unlike the other warfighting domains, cyber-threats will only continue to rise. When the war in Afghanistan is over, we will continue to fight in the cyber-domain with no end in sight. Time is critical. If we fail to adapt and prepare, we risk losing our next conventional war even before the first kinetic round is fired. In order for the U.S. to win in the cyber-domain, a new comprehensive approach and strategy is needed to build the cyber-warriors to defend it. More importantly, this new breed of warriors is going to be the foundation for the nation's security, and, ultimately its future success.

Conclusion

Cyberspace is a new frontier. It is and will continue to transform how we protect, defend and execute our nation's wars. Freedom of cyber-operations is a national interest. The U.S.'s ability to win conflicts in the cyber-domain hinges on the emerging workforce that will manage and operate the nation's military networks, critical infrastructure, and private sector and governmental networks. A full-scale sophisticated cyber-attack against a vulnerable network could virtually destroy every computer operating on it. The DOD's mission is to defend the nation and, during the 20th century,

it has done so by developing the best warfighters and combat equipment to conduct military actions on land, air and sea. In the 21st century, though, the U.S. military must not only defend its networks but also support the DHS to secure the nation's cyberspace as well. The only way to defend and win in cyberspace is to develop a highly trained cyber-workforce with the skills needed to detect and defend the network from attacks before they happen. We must allocate and authorize funding for recruiting, retaining and training cyber-professionals to help build the force needed for the 21st century. The resources to train this force would come at a fraction of the cost of the recovery cost associated with a catastrophic cyber-attack.

Even with the progress made in cyber-training, more is needed. Through this paper's assessment of the DOD's current training approaches and methods, the following recommendations will support the strategies to effectively operate and win a contested cyber-domain.

Recommendations

Training remains the most critical link for preparing the cyber-workforce of the 21st century. To meet the DOD's need for the thousands of highly skilled cyber-professionals, more advanced cyber-specialized training is needed. Given that the speed with which cyber's evolution outpaces the military's ability to effectively train all areas and specialties, the DOD should look into expanding the use of private and commercial providers to augment existing capabilities. Virtual labs and training venues provided by the private sector could be more adaptive in addressing the necessary specialized and specific training. In some cases, outsourcing may even generate a greater return on investment than in-house cyber-instructions, and even improve training from basic operation and maintenance of networking and IT equipment to focus

on countering real-world threats and vulnerabilities. Moreover, the DOD must also equalize training to include greater opportunities for the civilian cyber-workforce from those offered to the uniformed population. If the U.S. is serious about developing the best cyber-workforce, it must invest in doing so by offering programs that afford a greater spectrum of training across the larger population.

In addition to baseline and computing environment certifications, which currently serve as an indicator of proficiency, the DOD must mandate increased incorporation of cyber in warfighting exercises and wargames. While certification serves as a foundation, the benefits of evaluation conducted during realistic exercises and wargames will prove a more accurate indicator of cyber proficiency. Simulation tools, cyber-challenges, cyber-ranges and other capabilities must be distributed appropriately to support DOD training efforts.[49]

In addition, as cyber-attacks have risen over the past decade, so has the availability of automated security tools and systems. The DOD should acquire and field the next generation of cyber-prevention and detection tools to assist in the defense of the enterprise information system as well as the training needed to operate them. Hence, the DOD must expedite the modernization of the cyber enterprise, since the vulnerabilities associated with some of DOD's legacy systems are creating a risk by not being patched or scanned for security vulnerabilities; essentially, if one cannot patch or scan it, one cannot defend it. Finally, investments must be made in updating and replacing unsupportable legacy systems that create greater cyber-security vulnerabilities. This legacy equipment undermines the cyber workforce's ability to defend the network. This equipment creates an unacceptable risk that the traditional

cyber organizations are not prepared to assume. Network Enterprise Centers, Directorates of Information Management and installation communication units are only as good as the environment they work in.

Endnotes

[1] Jared Serbu, “DoD Building Cyber Workforce of the Future,” *FederalNewsRadio.Com*, September 19, 2012, http://www.federalnewsradio.com/885/3021032/DoD-building-cyber-workforce-of-the-future (accessed October 12, 2012), 2.

[2] Robert Turk and Shawn Hollingsworth, “Information Assurance: Army Prepares for Next Generation of Warfare,” *Army Communicator*, vol. 25, pp. 34-35, 2000.

[3] Mary Legere, "Cyber Domain and LandWarNet: Powering the Army,” panel discussion, Washington D. C, Association of the United States Army Conference, October 23, 2012, 2.

[4] J. Nicholas Hoover, “Cyber Attacks Becoming Top Terror Threat, FBI Says,” *Information Week*, February 01, 2012, http://www.informationweek.com/government/security/cyber-attacks-becoming-top-terror-threat/232600046 (accessed November 1, 2012), 1.

[5] Robert M. Gates, *Department of Defense Strategy for Operating in* Cyberspace (Washington, DC: U.S. Department of Defense, July 2011), 1.

[6] Ilan Berman, Vice President American Foreign Policy Council, Concerning the Iranian Cyber Threat to the U.S. Homeland Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Subcommittee on Counterterrorism and Intelligence, April 26, 2012, 1.

[7] Samantha Sais, “US Admits to Lack of Cybersecurity Professionals as War Drums Beat Louder”, *RT*, November 1, 2012, http://rt.com/usa/news/us-cyber-security-skills-702/ (accessed November 1, 2012), 1.

[8] "News Transcript: Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.” Defense.gov, October 11, 2012. Web December 10, 2012. Transcript.

[9] John G. Grimes, “Information Assurance Workforce Improvement Program,” (Washington, DC: Department of Defense, July 2011), 3.

[10] Amber Corrin, “Desperately Seeking Cybersecurity Pros,” *FCW*, October 26, 2012, http://fcw.com/Articles/2012/10/26/cyber-workforce.aspx?Page=1 (accessed November 7, 2012) 1.

[11] Ibid.

[12] Jared Serbu, "DoD Building Cyber Workforce of the Future," *FederalNewsRadio.Com*, September 19, 2012, http://www.federalnewsradio.com/885/3021032/DoD-building-cyber-workforce-of-the-future (accessed October 12, 2012), 2.

[13] Ibid.

[14] Ibid.

[15] John G. Grimes, "Information Assurance Workforce Improvement Program," (Washington DC, Department of Defense, Incorporating change 3 as of January 24, 2012), 12.

[16] Ibid, 19.

[17] Ibid, 19.

[18] Desmond A. Reid, Jr. Cyber Sentries: Preparing Defenders to Win in a Contested Domain, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, July 7, 2012), 2.

[19] Karen Evans and Frank Reeder, A Human Capital Crisis in Cybersecurity, Technical Proficiency Matters: A Report of the CSIS Commission on Cybersecurity for the 44th President, (Washington D.C.: Center of Strategic and International Studies, November 2010), v-vi.

[20] Ibid, 3-4.

[21] Daniel Castro, "The Role of Professional Certification in Securing Information Systems," October 14, 2009, http://itif.org/files/WM-2009-05-certification.pdf (accessed November 25, 2012), 1-2.

[22] Jim Gosler, "Cyberwarrior Shortage Threatens U.S. Security," *NPR Morning Edition*, July 19, 2010, http://npr.mobi/templates/transcript/transcript.php?storyId=128574055

[23] Jared Serbu, "Military Branches Refine Cyber Roles" *FederalNewsRadio.Com*, July 30, 2012, http://www.federalnewsradio.com/index.php?nid=851&sid=2969130 (accessed November 10, 2012), 1.

[24] Henry Keyon, "Air Force Emphasizes Skills Training for Cyber Personnel New Occupational Skills Category Helps Define Cyber Career Path," *Defense Systems*, January 27, 2012, http://defensesystems.com/articles/2012/01/27/air-force-emphasizes-skills-training-for-cyber-personnel.aspx (accessed January 8, 2013), 1.

[25] Amber Corrin, "Cyber Programs at a Glance," *FCW*, November 17, 2011, http://fcw.com/Articles/2011/11/28/FEAT-military-cyber-training-SIDE-overview.aspx?Page=2 (accessed November 29, 2012), 2.

[26] LtGen George J. Flynn, Concerning Operation in the Digital Domain: Organizing the Military Departments for Cyber Operations, Statement of Deputy Commandant for Combat Development and Integration before the House Armed Services Committee, September 23, 2010, 3.

[27] Amber Corrin, “Cyber Programs at a Glance,” *FCW*, November 17, 2011, http://fcw.com/Articles/2011/11/28/FEAT-military-cyber-training-SIDE-overview.aspx?Page=2 (accessed November 29, 2012), 2.

[28] Ibid.

[29] Amber Corrin, “Cyber Training No Longer Basic,” *FCW*, November 18, 2011, http://fcw.com/articles/2011/11/28/feat-military-cyber-training.aspx (accessed November 19, 2012)

[30] Jared Serbu, “Dod Building Cyber Workforce of the Future,” *FederalNewsRadio.Com*, September 19, 2012, http://www.federalnewsradio.com/885/3021032/DoD-building-cyber-workforce-of-the-future (accessed October 12, 2012), 2.

[31] William J. Lynn III, “Defending a New Domain the Pentagon's Cyberstrategy,” *Foreign Affairs*, September/October 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed December 12, 2012).

[32] Noah Shachtman, “Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack,” August 25, 2010, http://www.brookings.edu/opinions/2010/0825_pentagon_worm_shachtman.aspx (accessed November 2, 2012).

[33] Steven Beardsley, “Army Training Centers Incorporating Cyberthreats into Exercises at Brigade Level,” *Stars and Stripes*, October 28, 2012, http://www.stripes.com/news/army-training-centers-incorporating-cyberthreats-into-exercises-at-brigade-level-1.194941 (accessed December 1, 2012), 2.

[34] Ibid.

[35] LTG Rhett Hernandez, Concerning Digital Warrior: Improving Military Capabilities in Cyber Domain: Statement of Commander, U.S. Army Cyber Command/2nd Army before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, 112th Cong., 2nd sess., July 25, 2012, 6.

[36] Neil Gaudreau and Jeffrey Combs, “DOD Cyber Range,” *CHIPS* – September 2012, http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=4035 (accessed November 19, 2012), 1.

[37] Tech. Sgt Scott McNabb, “AF Competes in Second Cyber Flag,” November 30, 2012, linked from *United States Air Force Home Page* at “News,” http://www.af.mil/news/story.asp?id=123328060, (accessed December 4, 2012).

[38] Jared Serbu, “DOD Building Cyber Workforce of the Future,” *FederalNewsRadio.Com*, September 19, 2012, http://www.federalnewsradio.com/885/3021032/DoD-building-cyber-workforce-of-the-future (accessed October 12, 2012), 2.

[39] Desmond A. Reid, Jr. Cyber Sentries: Preparing Defenders to Win in a Contested Domain, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, July 7, 2012), 9.

[40] Jim Gosler, “Cyberwarrior Shortage Threatens U.S. Security,” *NPR Morning Edition*, July 19, 2010, http://npr.mobi/templates/transcript/transcript.php?storyId=128574055,

[41] Jared Serbu, “DoD Building Cyber Workforce of the Future,” *FederalNewsRadio.Com*, September 19, 2012, http://www.federalnewsradio.com/885/3021032/DoD-building-cyber-workforce-of-the-future (accessed October 12, 2012), 2.

[42] Barack Obama, Comprehensive National Cybersecurity Initiative (Washington DC: The White House, May 2, 2010), 5.

[43] Ibid.

[44] Tom Gjelten, “Cyberwarrior Shortage Threatens U.S. Security,” *NPR*, July 19, 2010, http://www.npr.org/templates/story/story.php?storyId=128574055

[45] The National Board of Information Security Examiners Home Page, https://www.nbise.org/uscc/he (accessed December 5, 2012).

[46] John G. Grimes, “Information Assurance Workforce Improvement Program,” (Washington DC, Department of Defense, Incorporating change 3 as of January 24, 2012, 22.

[47] Jared Serbu, “DoD Building Cyber Workforce of the Future,” *FederalNewsRadio.Com*, September 19, 2012, http://www.federalnewsradio.com/885/3021032/DoD-building-cyber-workforce-of-the-future (accessed October 12, 2012), 1.

[48] News Transcript: Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.” Defense.gov, October 11, 2012. Web December 10, 2012. Transcript

[49] Desmond A. Reid, Jr. Cyber Sentries: Preparing Defenders to Win in a Contested Domain, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, July 7, 2012), 22.